



February 2002
OSD(HA), TMA eBPS

HIPAA - Privacy

TRICARE Management Activity, Electronic Business Policy & Standards, February 2002

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

Highlights

- ↓ HIPAA Privacy Overview
- ↓ HIPAA Privacy Rule
- ↓ Penalties For Non-Compliance
- ↓ Who Must Comply With HIPAA?
- ↓ What Information Is Protected?
- ↓ Why Is HIPAA Privacy Important To The Patient?
- ↓ How Do I Get Started At The MTF Level?

Overview

Each time a patient sees a doctor, is admitted to a hospital, goes to a pharmacist or sends a claim to a health plan, a record is made of his/her confidential health information. In the past, family doctors and other health care providers protected the confidentiality of those records by sealing them away in file cabinets and refusing to reveal them to anyone else. Today, the use and disclosure of this information is protected by a patchwork of state laws, leaving gaps in the

protection of patients' privacy and confidentiality.

Congress recognized the need for national patient record privacy standards in 1996 when they enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The law included provisions designed to save money for health care businesses by encouraging electronic transactions, but it also required new safeguards to protect the security and confidentiality of that

information. The law instructed Congress to pass comprehensive health privacy legislation. When Congress did not enact such legislation after three years, the law required the Department of Health and Human Services (HHS) to craft such protections by regulation.

More information can be found at
<http://www.hhs.gov/ocr>.

HIPAA Privacy Rule

The Privacy Rule provides the first comprehensive federal protection for the privacy of health information. All segments of the health care industry have expressed their support for the objective of enhanced patient privacy in the health care system. At the same time, HHS and most parties agree that privacy protections must not interfere with a patient's

access to or the quality of health care delivery.

In November 1999, HHS published proposed regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records. More than 52,000 communications were received from the public during an extended comment period. HHS issued a final rule in

December 2000 that made significant changes in order to address issues raised by those comments. After another comment period, the rule was allowed to take effect on April 14, 2001.

The Military Health System must be in compliance with the HIPAA Privacy rule by April 14, 2003.

Penalties For Non-Compliance

The rule is enforced by the HHS Office of Civil Rights (OCR). Penalties for non-compliance with the HIPAA Privacy rule may apply to the individual violator, commander or organization. Civil monetary penalties will be incurred on a per person, per violation basis. Fines and prison terms may result for misuse of patient information with knowledge and intent.



Electronic Business Policy &
Standards

**HIPAA
PROGRAM OFFICE**

Skyline 6, Suite 817
5109 Leesburg Pike
Falls Church, VA
22041-3206

PHONE:
703- 681-5611

FAX:
703-681-8845

E-MAIL:
hipaamail@tma.osd.mil

We're on the Web!

See us at:

[www.tricare.osd.mil/
hipaa](http://www.tricare.osd.mil/hipaa)



HIPAA Privacy - Who, What, Why & How

The purpose of the HIPAA Privacy Rule is to prevent inappropriate use and disclosure of individuals' health information. It is not a one-time implementation project. HIPAA entails ongoing responsibilities that must be incorporated into MHS culture and business processes.

Who Must Comply With HIPAA?

All health plans, health care clearinghouses and health care providers who conduct certain financial and administrative transactions electronically must comply with HIPAA. TRICARE, the MTFs, clinicians, the managed care support contractors (MCSCs) and subcontractors as well as other business associate relationships fall within these categories.

What Information is Protected Under HIPAA?

Individually identifiable health information, including demographics, is protected under HIPAA. This protected health information (PHI) can be in electronic, paper or verbal form. It is not limited to documents contained in the official medical record. Consent must be obtained from the patient to use or disclose PHI for treatment, payment and health care operations (TPO). Uses and disclosures related to TPO are described in an organization's Notice of Privacy Practices. All other uses and disclosures require an authorization.

Health information covered by the rule generally may not be used for purposes not related to health care without explicit authorization from the individual. In general, disclosures of information will be limited to the minimum necessary for the purpose of the disclosure. However, this provision does not apply to the disclosure of a medical record for treatment purposes because physicians, specialists and other providers need access to the full record to provide quality care.

Why Is HIPAA Important To The Patient?

HIPAA increases the patient's control over his/her health information. The patient has the right to:

- § A written notice of information practices from health plans and providers;
- § Access, inspect and obtain a copy of PHI;
- § Request amendment to or correction of records;
- § Obtain an accounting of disclosures;
- § Request restrictions on uses and disclosures;
- § Accommodation of reasonable communications requests;
- § Complain to the covered entity and to HHS.

How Do I Get Started At The MTF Level?

- § Designate MTF Privacy Officer
- § Train the workforce
- § Review the DoD HIPAA Privacy Regulation
- § Map your patient information flow
- § Conduct gap analyses and adjust policies/procedures
- § Institute Notice of Privacy Practices, record patient consent and institute authorization forms
- § Establish patient privacy complaint and inquiry procedure
- § Assess compliance using TMA tool